Fairoaks IT
Cybersecurity | AI Advisory | Managed IT | Cloud

2026 edition

Before You Hire (or Fire) Your IT Company

The Healthcare Practice's Q&A Guide

Straight answers for owners, administrators and office managers at medical, dental and behavioral health practices, plus five tools you can put to work this week.

Soteria Award winner
Most Trusted MSP in North America

Prepared by **Adam Crossley, CEO, Fairoaks IT**	Established **1991, independent and owner-led**
Serving **Eastern Massachusetts, Rhode Island and the Charlotte, NC area**	Offices **Franklin, MA and Belmont, NC**

What's inside

The 2-minute scorecard	3
Is it time to fire your IT company?	4
Patient care and uptime	5
HIPAA and compliance	7
Security and fraud	10
Cost, contracts and switching	12
10 questions to ask before you sign	15
Tool 1: Risk analysis starter checklist	16
Tool 2: BAA tracker	17
Tool 3: Breach response checklist	18
Tool 4: Staff onboarding and offboarding	19
Tool 5: Patient email and texting policy	20
What happens in an assessment	21
About Fairoaks IT	22

From the desk of Adam Crossley

Every practice I talk to wants the same thing from technology: for it to disappear. The EHR should open, the front desk should check patients in, the imaging computer should talk to the chart, and nobody should have to think about any of it.

When that doesn't happen, it shows up fast: a waiting room that backs up, a provider charting at night because the system was down at noon, or a "patient" email that turns out to be the start of a breach.

And then there's HIPAA. Most practices know they need a risk analysis, written policies and a business associate agreement with every vendor that touches patient data. Fewer are confident theirs are current, and the rules may be about to get stricter.

The most common story I hear isn't about a hacker. It's about a practice owner who is paying an IT company and still managing every problem personally.

So we wrote this guide to give you straight answers. Whether you're hiring your first IT company, thinking about firing the one you have, or just want to know where you stand, you'll find:

- a 2-minute scorecard to see where your IT stands today
- the warning signs that it's time to make a change
- plain-English answers about uptime, HIPAA and security
- 10 questions to ask any IT company before you sign
- five tools you can copy and use this week

No scare tactics and no jargon. If something in here raises a question, call us. If we're not the right fit for you, we'll tell you.



Adam Crossley
CEO, Fairoaks IT

Start here

The 2-minute scorecard: is your IT built for a healthcare practice?

Check yes only if you're sure. "I think so" counts as no. That isn't us being tough; it's how HHS or an insurance carrier will see it after a breach.

1	When someone calls for IT help, a real person starts on it within minutes, not hours.	☐ Yes	☐ No
2	Your IT company has signed a business associate agreement with your practice.	☐ Yes	☐ No
3	Your HIPAA security risk analysis is written down and was reviewed in the last year.	☐ Yes	☐ No
4	Every login to email, the EHR and remote access uses multi-factor authentication.	☐ Yes	☐ No
5	Laptops and any device holding patient information are encrypted.	☐ Yes	☐ No
6	Patient records and practice data are backed up where ransomware can't reach them, and were test-restored in the last 90 days.	☐ Yes	☐ No
7	You have written downtime procedures, so the front desk can keep seeing patients if systems go down.	☐ Yes	☐ No
8	Imaging equipment and medical devices are on their own network segment.	☐ Yes	☐ No
9	Every staff member has their own login. Nobody shares a front-desk password.	☐ Yes	☐ No
10	Staff get security training and phishing tests at least once a year.	☐ Yes	☐ No
11	You have a written breach response plan, including HHS notification timelines.	☐ Yes	☐ No
12	Your IT costs are predictable, and you know exactly what is and isn't included.	☐ Yes	☐ No

11 to 12 yes

You're in good shape. Use the rest of this guide to keep it that way.

8 to 10 yes

A solid foundation with real gaps. Fix the no's this quarter, starting with your BAA, risk analysis and MFA.

5 to 7 yes

You're carrying more risk than you probably realize. One bad email or failed server could close your doors for days.

0 to 4 yes

Your IT is running on luck. Let's talk before the luck runs out.

The “fire” part

Is it time to fire your IT company? Eight warning signs

Plenty of organizations already pay for IT support and still aren’t getting it. If three or more of these sound familiar, it’s time for a serious conversation, either with your current provider or with a new one.

1

You’re still chasing them.

You pay for IT support, and you’re still the one following up, escalating and checking whether anything got done.

2

The same problems keep coming back.

They fix the symptom and move on. A week later it’s back, and nobody has looked for the cause.

3

You have to explain your EHR.

If you’ve had to explain what athenahealth, Dentrix or Open Dental is, they’re learning on your dime.

4

Nobody can tell you if your backups work.

Ask when they last did a test restore of your practice data. A vague answer is the answer.

5

They’ve never offered a BAA.

If they can reach patient information, HIPAA says they need one. Not offering it is a red flag.

6

They go quiet on HIPAA.

Ask about your risk analysis or policies, and suddenly nobody has an answer.

7

You only hear from them when something breaks.

Or when the invoice shows up. No planning, no reviews, no recommendations until there’s an emergency.

8

Everything lives in their head.

If you asked for your admin passwords and network documentation today, could you get them? If not, they control your IT, not you.

> **Worried about disrupting patient care during a switch?** That fear keeps a lot of practices stuck with IT support they don’t like. Page 14 walks through what a clean switch looks like, step by step.

Chapter 1

Patient care and uptime

When technology stops, patients wait. This chapter covers keeping systems fast, devices safe and the practice running when something fails.

How do we keep the EHR fast during patient hours?

Most slowdowns come from the pieces around the EHR, not the EHR itself:

- Computers past their prime, especially at the front desk and in exam rooms
- A congested network or weak Wi-Fi in exam rooms
- An overdue server for on-premise systems like Dentrix, Eaglesoft or Open Dental
- An internet connection too small for a cloud EHR like athenahealth

Keep computers on a replacement schedule, monitor the network and internet, add a backup internet connection if your EHR lives in the cloud, and schedule updates outside patient hours. When the problem is on the vendor's side, your IT provider should open the case and stay on it.

What should happen if systems go down?

Your team should already know. Written downtime procedures tell the front desk how to check patients in, tell clinicians how to document, and say who calls whom. Keep paper forms and a printed schedule ready, and practice once a year. Then make sure the recovery side is real: backups that ransomware can't reach, tested restores and a provider that starts fast. Our average time to start on a support issue is under 12 minutes.

Chapter 1, continued

Patient care and uptime

Quick win

Print next week's schedule every Friday and keep downtime forms at the front desk. It turns an outage into an inconvenience.

How should imaging equipment and medical devices be handled?

On their own network segment. Imaging systems and other devices often run older software that can't be updated like office computers, so separating them limits what an attacker or a virus can reach. Vendor remote access should be controlled and turned on only when needed, and every connected device should be documented: what it is, where it connects and who supports it.

Cloud EHR or a server in the office?

It depends on your software. Cloud systems take servers off your plate but depend on a reliable internet connection. Many dental and specialty systems still run on an office server, which needs proper backup, security and replacement planning. Some vendors offer hosted versions too. Compare the options side by side, with costs, before anything moves.

How do providers work securely from home or another location?

With company-managed devices, secure remote access and multi-factor authentication on every login, so patient information never lives on personal computers. Multi-location practices should have the same standards everywhere, with each location connected securely to the EHR and phones.

Chapter 2

HIPAA and compliance

HIPAA expects real safeguards, documented and current. This chapter covers what the rules require today and what may be coming.

What does HIPAA require from a practice's IT?

The Security Rule requires administrative, physical and technical safeguards for electronic patient information, including:

- A security risk analysis, and a plan to manage the risks it finds
- Written policies and workforce training
- Access controls, so people see only what they need
- Audit controls and protection against tampering
- Secure transmission of patient information
- Contingency planning, including backups
- Business associate agreements with vendors who handle patient data

All of it needs to be documented and kept current.

Does our IT company need to sign a BAA?

Yes. Any IT provider that can access systems holding patient information is a business associate, and you need a signed business associate agreement before they start. Fairoaks IT signs BAAs with our healthcare clients. Track every vendor that touches patient data with the tracker on **page 17**.

60 days

The outside limit for notifying patients after discovering a breach of unsecured patient information.

What is a security risk analysis, and how often do we need one?

It identifies where patient information lives in your practice, the threats and weaknesses that could expose it, and how you're addressing each one. HIPAA requires it, and it's the first document regulators ask for after a breach. The current rule doesn't set a fixed schedule, but review it regularly and whenever systems change; most practices review it yearly. Tool 1 on page 16 gets you started.

Is the Security Rule changing?

A major update has been proposed but not finalized. In December 2024, HHS proposed making protections like multi-factor authentication and encryption mandatory, and adding requirements like an asset inventory, vulnerability scanning and penetration testing. As of fall 2026, it hadn't been finalized, and HHS now targets July 2027 for final action. The current rule is what's enforced, but the proposed protections are good practice now.

HIPAA and compliance

Worth knowing
HIPAA doesn't cover veterinary records. But vet practices hold client and payment data that state laws can protect.

What do we have to do after a breach?

Act fast and follow your written plan. Affected patients must be notified without unreasonable delay and no later than 60 days after discovery. Breaches affecting 500 or more people must also be reported to HHS within 60 days, with notice to prominent media when 500 or more residents of a state are affected; smaller breaches are reported to HHS annually. State laws can add requirements. The checklist on **page 18** walks through it.

Can we email or text patients?

Yes, with safeguards. Messages containing patient information should be encrypted, and patients should be told about the risks if they ask for unencrypted messages. Use a portal or secure messaging for anything sensitive, and write down the rules so everyone follows them the same way. Start with the policy on **page 20**.

Do you provide policies and training?

Yes. We help practices create written HIPAA security policies and set up an easy way for every employee to acknowledge them, and most of our plans include staff security training and phishing simulations.

Chapter 3

Security and fraud

Healthcare is one of the most targeted industries. This chapter covers how attackers get in and the basics that stop most of them.

Why are practices targeted?

Because patient records are valuable and practices can't afford downtime. A practice that can't see patients is under enormous pressure to pay a ransom, and health records can be sold or used for identity and insurance fraud. The 2024 Change Healthcare attack also showed how one breach at a vendor can disrupt practices nationwide.

What security controls should every practice have?

- Multi-factor authentication on email, the EHR and remote access
- Encryption on laptops and in transit
- Endpoint protection on every computer and server
- Email filtering for phishing and lookalike domains
- Security updates on a schedule someone checks
- Backups that ransomware can't reach, test-restored
- Staff training with phishing simulations
- Medical devices on their own network segment

At Fairoaks IT, security updates, endpoint protection and 24/7 monitoring come standard. Most of our plans add staff training and phishing simulations, and our advanced security option adds a 24/7 security operations center.

Chapter 3, continued

Security and fraud

Software we support
athenahealth, eClinicalWorks, NextGen, Dentrix, Eaglesoft, Open Dental, SimplePractice, TherapyNotes, AVImark, Cornerstone and Microsoft 365.

How should we handle staff who leave or change roles?

Remove access the day someone leaves, from every system: the EHR, email, practice management, patient portal, remote access and shared accounts. When people change roles, adjust access to match. Shared front-desk logins make it impossible to know who did what, so give each person their own. Use the checklist on **page 19**.

Can staff use AI tools with patient information?

Only tools approved for patient data, which generally means a business-grade tool covered by a business associate agreement. Free and personal AI accounts may keep what your team types in, so patient names, records and images never go into them. Name the approved tools in writing.

What do cyber insurance carriers require?

Most ask about multi-factor authentication, endpoint detection and response, tested backups that can't be altered, security training and timely patching. Many overlap with HIPAA's safeguards. Make sure every yes on the application is true. Your insurance agent has the final word on your policy.

Chapter 4

Cost, contracts and switching

This is where most IT relationships go right or wrong: how IT companies charge, what to watch for in a contract and how to switch cleanly.

How do IT companies charge, and which model puts the risk on you?

There are three common ways:

- **Time and materials (break-fix):** you pay by the hour when something breaks. It looks cheap until a bad month, and the provider makes more money when your systems have more problems.
- **Managed services:** a predictable monthly fee, usually per user or per device, covering support, maintenance and monitoring. The provider does better when your systems run well.
- **Software vendor support:** help with one application only. Useful, but it stops at the edge of their software.

Some form of managed services almost always makes the most sense. Our IT Buyer's Guide covers each model, and typical industry pricing, in detail.

What should be included in the monthly fee, and what's usually extra?

Every provider draws the line in a different place, so get it in writing. Monthly plans typically cover support for your users, monitoring and maintenance, security tools, backup management and Microsoft 365 administration. Hardware, software licenses and subscriptions are almost always extra, and bigger projects are usually quoted separately.

Ask specifically about onsite time, after-hours help, adding and removing users, and new hardware setup. At Fairoaks IT, we explain every cost up front.

Chapter 4, continued

Cost, contracts and switching

Get it in writing

Your passwords, documentation and data belong to you, no matter who your IT provider is.

What contract terms should make us nervous?

- **Vague scope:** "unlimited support" with no definition of what's covered
- **Buried exclusions:** especially onsite visits, after-hours work and anything labeled a "project"
- **Open-ended project billing:** hourly work with no estimate or cap
- **No way out:** long terms with no remedy if service is poor
- **Unclear ownership:** no written answer on who owns your passwords, documentation and data if you leave

That last one matters most. Your admin passwords, network documentation and data belong to you. Any provider who hesitates to say so in writing is telling you something.

How long should an IT agreement be, and what if it isn't working?

Multi-year agreements are common, and they can work in your favor: they lock in your rate and give the provider reason to invest in your environment.

What matters is what happens if things aren't working. Ask every provider two questions: what happens if you don't deliver, and how are price increases handled? Get both answers in writing. Ours are spelled out in our agreement, and we'll walk you through every page before you sign.

Before you sign

Ask every provider to walk you through their onboarding plan, step by step.

How do we switch IT providers without disrupting patient care?

With a plan built around your schedule. A clean switch looks like this:

1. Discovery before anything changes: every system, password, license and vendor documented
2. A coordinated handoff from your current provider. Nobody flips a switch on a Friday afternoon.
3. Onboarding scheduled outside patient hours, with a signed BAA before work begins
4. The biggest risks fixed first, like backups and multi-factor authentication
5. One named point of contact and weekly check-ins until onboarding is done

If a provider can't walk you through their onboarding plan before you sign, keep looking.

Should we just hire an IT person instead?

For most practices, one internal hire is the riskier choice. One person can't be an expert in networks, security, the EHR, imaging and HIPAA at once, and they take vacations and sick days. When they leave, what they know leaves with them.

If you already have a good IT person, the best answer may be both. Co-managed IT gives them a full team behind them, without replacing them.

The "hire" part

10 questions to ask any IT company before you sign

Bring these to every meeting. The answers tell you more than any proposal, and a good provider will be glad you asked.

1 Will you sign our business associate agreement?

A good answer: "Yes," before any work begins.

2 How fast does a real person start on an issue?

A good answer: A specific average they track and report. Ours is under 12 minutes.

3 What isn't included in the monthly fee?

A good answer: A written list of exclusions, offered without hesitation.

4 Which EHR and practice systems do you support today?

A good answer: Names you recognize, like athenahealth, Dentrix or Open Dental, without you explaining them.

5 Can you perform our HIPAA risk analysis and help with policies?

A good answer: Yes, with a plan to fix what it finds, not just a report.

6 How do you handle imaging equipment and medical devices?

A good answer: A plan to segment them and control vendor remote access.

7 When did you last test-restore a client's backup?

A good answer: A recent date and what they restored. Not "the backups run every night."

8 How will you onboard us without disrupting patient care?

A good answer: A documented plan scheduled outside patient hours, with a point of contact and regular check-ins.

9 If we leave, do we get all our passwords, documentation and data?

A good answer: "Yes, it's yours," and they'll put it in writing.

10 What happens if you don't deliver, and can I talk to a practice you support?

A good answer: A clear, written answer, and references from practices like yours.

> **How we answer them:** we sign business associate agreements, our average time to start on an issue is under 12 minutes, the software list is on **page 11**, we perform risk analyses and penetration testing, and our agreement spells out what's included before you sign.

Tool 1

Security risk analysis starter checklist

Print and use

Use this to start a risk analysis or check an existing one. Every box should point to something written down.

Practice	Done by	Date	Next review

Where patient information lives

- [ ] EHR and practice management system
- [ ] Imaging systems and medical devices
- [ ] Email, file shares and Microsoft 365
- [ ] Laptops, phones and tablets
- [ ] Backups, and where they're stored
- [ ] Vendors and cloud services that store or reach patient data

Threats and weaknesses

- [ ] Phishing and stolen passwords
- [ ] Ransomware and malware
- [ ] Lost or stolen devices
- [ ] Former staff who still have access
- [ ] Outdated software on devices that can't be updated

What you're doing about each

- [ ] Multi-factor authentication and encryption
- [ ] Endpoint protection and security updates
- [ ] Backups that are tested
- [ ] Access reviews and same-day offboarding
- [ ] Staff training and phishing tests

Tool 2

Business associate agreement tracker

Fill in

List every vendor that creates, receives, stores or transmits patient information for you, and confirm each has a signed BAA.

Vendor	What they do with patient data	BAA signed (date)	Review date
IT provider	Supports systems holding patient data		
EHR or practice management vendor	Stores patient records		
Billing or clearinghouse	Submits claims		
Email and cloud storage	Stores messages and files		
Backup provider	Stores copies of your data		
Patient communication or reminders	Sends texts or emails		
Transcription, answering or other services			

Tool 3

Breach response checklist

Print and use

Fill in the contacts now and keep a printed copy where you can reach it if systems are down. This is a starting point, not legal advice.

Incident lead	IT provider phone	Insurance carrier phone	Attorney phone

First hour

- [ ] Disconnect affected computers from the network, but leave them powered on
- [ ] Call your IT provider
- [ ] Call your cyber insurance carrier before hiring outside help
- [ ] Start a written log of what happened and when

First days

- [ ] Determine what patient information was involved and whether it was encrypted
- [ ] Call your attorney
- [ ] Follow your downtime procedures so patient care continues

Within 60 days of discovery

- [ ] Notify affected patients
- [ ] If 500 or more people were affected, report to HHS and notify prominent media where required
- [ ] Check state breach laws for additional notices

Afterward

- [ ] Log breaches under 500 people and report them to HHS within 60 days after the end of the year
- [ ] Update your risk analysis and policies with what you learned

Tool 4

Staff onboarding and offboarding checklist

Print and use

Use one per person, including temps, students and contractors who had system access.

Name	Role	Start date	Last day

Before day one

- [ ] Create an individual login for every system, with multi-factor authentication
- [ ] Grant only the EHR and system access the role needs
- [ ] Provide a company device, never a personal computer
- [ ] Complete HIPAA and security training before access starts
- [ ] Have them read and acknowledge your security policies

On the last day

- [ ] Disable accounts and sign them out of every session
- [ ] Remove EHR, practice management and patient portal access
- [ ] Remove company email and data from personal phones
- [ ] Collect laptops, keys, badges and tokens
- [ ] Change any shared passwords they knew
- [ ] File this checklist with your HIPAA records

Tool 5

Patient email and texting policy starter

Copy and use

Fill in the blanks, share it with every provider and staff member, and add it to your HIPAA policies.

_____ Patient Communication Policy

1. We send patient information by email or text only through _____, our approved secure messaging tool or patient portal.
2. Messages containing patient information are encrypted. If a patient asks for unencrypted messages, we explain the risks and document their request.
3. Appointment reminders contain only the minimum information needed: no diagnoses, results or treatment details.
4. Staff never use personal email, personal phones or personal messaging apps for patient communication.
5. We verify a patient's identity before discussing their information by phone or replying to a new email address.
6. Unexpected attachments or links from patients or vendors are forwarded to _____ before anyone opens them.
7. Questions about this policy go to _____.

_____ _____

Approved by Date

Next step

What happens in a Fairoaks IT assessment

We look at your technology the way you'd look at a new patient: all of it, with a written report at the end. It starts with a discovery call.

> **Schedule a discovery call**
> fairoaksit.com/discoverycall

What we review

- Network, firewall and Wi-Fi in exam rooms
- Servers and your EHR setup
- Imaging and front-desk devices
- Microsoft 365 and email security
- Backups, and whether they can actually be restored
- Security tools and updates
- Your HIPAA risk analysis, policies and BAAs
- Cyber insurance requirements

What you get

A plain-English report on what's working, what's at risk and what to fix first, with quick wins called out and monthly support kept separate from one-time projects. No scare tactics, just facts. If we're not the right fit, we'll tell you.

What you can count on

Help in minutes, not hours. Our average time to start on a support issue is under 12 minutes, with live support during business hours and after-hours support available.

No surprises. Before you sign, you'll know exactly what's included, what isn't and how every cost works. It's all in writing, and we'll walk you through every page.

Accountable at the top. Fairoaks IT is owned and run by Tom and Adam Crossley. If something isn't right, the people who own the company are the people who answer for it.

From our Client Bill of Rights:

- Answers to your questions in plain English
- All costs explained up front, with no hidden fees
- A single point of contact for every technology issue, including help with your other vendors
- Your request acknowledged within an hour

Who we are

About Fairoaks IT

An independent, owner-led managed IT and cybersecurity company. Tom Crossley founded Fairoaks IT in 1991, and he and his son, Adam Crossley, own and run it today.

We support medical, dental, behavioral health and other healthcare practices across Eastern Massachusetts, Rhode Island and the Charlotte, NC area from offices in Franklin, MA and Belmont, NC.

Soteria Award winner
Most Trusted MSP in North America

Microsoft Partner. Certified Trust Level 2 IT provider. As seen on MarketWatch, Newsmax, Business Insider and FOX 28.

<12 min Average time to start on a support issue	**99.98%** Average network uptime for fully managed clients	**98%** End-user satisfaction

What our clients say

"Fairoaks IT has always been there for us when we've needed them. If a problem can't be solved remotely, they head right over in person to get it fixed. We love how responsive they are and the knowledge of their staff."



Taylor MacElhiney
Billing Coordinator, Boston Orthotics

"Each person from Fairoaks IT has been pleasant, professional, and clear on each step that's been taken... We commend you for creating such an environment in your IT business."

NB

Nancy Borowy
Milford Franklin Counseling Services, Inc.

"It is a mean world out there in all respects, and Fairoaks IT have diligently kept us informed and trained to avoid click bait and phishing emails."



Rob English
Owner, Chemical Solutions

"Tom and Adam are always accessible too, so when we do need to review our account and service, you are available to us."



Kevin Lagasse
Executive Vice President, The Lagasse Group

Ready for straight answers about your IT?

Schedule a discovery call: a straightforward conversation about your practice and what isn't working. No pitch and no pressure. If we're not the right fit, we'll tell you.

fairoaksit.com/discoverycall

Franklin, MA

1000 Franklin Village Dr, Suite 303
Franklin, MA 02038
(774) 222-5500

Eastern Massachusetts and Rhode Island

Belmont, NC

32 North Main Street, Suite 206
Belmont, NC 28012
(704) 440-9016

The Charlotte, NC area

fairoaksit.com/industries/healthcare

Fairoaks IT
Cybersecurity | AI Advisory | Managed IT | Cloud

Soteria Award winner: Most Trusted MSP in North America

© 2026 Fairoaks IT. General information, not legal advice.